IX kadencja



KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 114)**

z dnia 12 lipca 2023 r.

Pełny zapis przebiegu posiedzenia

Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 114)

12 lipca 2023 r.

Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, obradująca pod przewodnictwem posła **Grzegorza Napieralskiego (KO)**, zastępcy przewodniczącego Komisji, zrealizowała następujący porządek dzienny:

– rozpatrzenie i zaopiniowanie dla Komisji do spraw Kontroli Państwowej Sprawozdania z działalności Najwyższej Izby Kontroli w 2022 roku (druk nr 3434) w zakresie działania Komisji;

– rozpatrzenie Informacji Najwyższej Izby Kontroli o wynikach kontroli „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości".

W posiedzeniu udział wzięli: **Paweł Lewandowski** podsekretarz stanu w Ministerstwie Cyfryzacji wraz ze współpracownikami, **Tomasz Sordyl** pełniący obowiązki dyrektora Departamentu Porządku i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli wraz ze współpracownikami, **insp. Michał Pudło** zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości Komendy Głównej Policji, **Sebastian Kondraszuk** kierownik Działu CERT Polska w Naukowej i Akademickiej Sieci Komputerowej oraz **Joanna Karczewska** członek Stowarzyszenia ISACA Warszawa. W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Adrian Konefał** i **Wioletta Więciorkowska** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Grzegorz Napieralski (KO):

Witam bardzo serdecznie. Otwieram posiedzenie Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii.

Stwierdzam kworum. Witam bardzo serdecznie posłów oraz gości uczestniczących w posiedzeniu. Na samym początku pragnę powitać pana ministra...

Myślałem, że coś się zmieniło… Chciałem przywitać ministra, a to pan poseł… OK.

Na samym początku chciałbym bardzo serdecznie powitać pana ministra Pawła Lewandowskiego, podsekretarza stanu w Ministerstwie Cyfryzacji. Witam panie ministrze. Witam również bardzo serdecznie zastępcę dyrektora Departamentu Cyberbezpieczeństwa – pan Marcin Wysocki jest z nami. Dzień dobry, panie dyrektorze. Komendę Główną Policji reprezentuje inspektor Michał Pudło, zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości. Witam pana bardzo serdecznie. Najwyższą Izbę Kontroli reprezentuje pani Agnieszka Bernaś-Coşkun, wicedyrektor Departamentu Administracji Publicznej. Dzień dobry, pani dyrektor. Pełniący obowiązki dyrektora Departamentu Porządku i Bezpieczeństwa Wewnętrznego, pan Tomasz Sordyl. Dzień, dobry, panie dyrektorze. Główny specjalista kontroli państwowej w Departamencie Porządku i Bezpieczeństwa Wewnętrznego, pan Adam Zakrzewski… Nie dotarł. Naukowa i Akademicka Sieć Komputerowa – Sebastian Kondraszuk, kierownik Działu CERT Polska. Członek Stowarzyszenia ISACA Warszawa, pani Joanna Karczewska, która zawsze jest z nami. Witam panią Joannę bardzo serdecznie. Dziękuję za przybycie.

Porządek dzisiejszego posiedzenia przewiduje w punkcie pierwszym rozpatrzenie i zaopiniowanie dla Komisji do Spraw Kontroli Państwowej Sprawozdania z działalności Najwyższej Izby Kontroli w roku 2022 (druk nr 3434) w zakresie działania Komisji. W punkcie drugim – rozpatrzenie informacji Najwyższej Izby Kontroli o wynikach

kontroli „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości”. Czy są uwagi do porządku dziennego? Wobec niezgłoszenia uwag do porządku dziennego stwierdzam jego przyjęcie.

Przechodzimy do rozpatrzenia punktu pierwszego. Marszałek Sejmu zgodnie z artykułem 126 ust. 4 regulaminu Sejmu skierowała w dniu 4 lipca bieżącego roku przedstawione przez prezesa Najwyższej Izby Kontroli sprawozdanie z działalności Najwyższej Izby Kontroli w roku 2022 (druk nr 3434) do Komisji do Spraw Kontroli Państwowej w celu rozpatrzenia i zaopiniowania. Jednocześnie marszałek Sejmu skierowała to sprawozdanie do pozostałych komisji sejmowych w celu rozpatrzenia w swoim zakresie działania oraz przedstawienia uwag i wniosków do Komisji do Spraw Kontroli Państwowej w terminie do 13 lipca 2023 roku. O zabranie głosu poproszę przedstawiciela Najwyższej Izby Kontroli. Bardzo proszę.

Pełniąca obowiązki wicedyrektor Departamentu Administracji Publicznej Najwyższej Izby Kontroli Agnieszka Bernaś-Coşkun:

Agnieszka Bernaś-Coşkun, pełniąca obowiązki wicedyrektora Departamentu Administracji Publicznej.

Szanowny panie przewodniczący, Wysoka Komisjo, realizując ustawowy obowiązek, chciałam przedstawić Wysokiej Komisji sprawozdanie z działalności Najwyższej Izby Kontroli w 2022 roku. Najwyższa Izba Kontroli w 2022 roku przeprowadziła 1896 kontroli jednostkowych w 1558 podmiotach w ramach 180 tematów. W wyniku tych kontroli NIK sformułowała 5102 wnioski pokontrolne, w tym 83,4% wniosków zostało przyjętych do realizacji. Wymiernym efektem kontroli Najwyższej Izby Kontroli w 2022 roku było zidentyfikowanie finansowych lub sprawozdawczych skutków nieprawidłowości w wysokości ponad 20 mld zł, w tym około 9,2 mld zł kwot wydanych z naruszeniem prawa, prawie 10 mln zł kwot, które w wyniku kontroli zostały lub zostaną pozyskane lub zaoszczędzone oraz ujawnione finansowe skutki nieprawidłowości na szkodę budżetu Unii Europejskiej na kwotę ponad 166 mln zł.

Po kontrolach sformułowano 80 wniosków de lege ferenda, w tym 60 dotyczących propozycji zmian ustawowych. Zrealizowanych zostało 6 wniosków, a 4 były w trakcie realizacji. W latach 2020–2022 NIK sformułowała łącznie 271 wniosków de lege ferenda, z których 24 zostały zrealizowane, a 22 pozostają nadal w trakcie realizacji. W 2022 roku NIK rozpatrzyła ponad 5,5 tys. wniosków o kontrolę i skarg obywatelskich. Zdecydowana większość skarg została złożona przez osoby fizyczne, głównie w zakresie administracji publicznej, gospodarki i finansów publicznych. Parlamentarzyści złożyli 88 wniosków o przeprowadzenie kontroli. Było to 2,6% ogólnej liczby spraw.

Do właściwych organów w 2022 roku skierowano łącznie 250 zawiadomień o podejrzeniu popełnienia przestępstw lub wykroczeń, a także innych czynów, za które przewidziana jest odpowiedzialność ustawowa, w tym 153 zawiadomienia do prokuratury. NIK skierowała do rzeczników dyscypliny finansów publicznych 85 zawiadomień o naruszeniu dyscypliny finansów publicznych, a w ramach współpracy z Sejmem NIK przedłożyła analizę wykonania budżetu państwa i założeń polityki pieniężnej w 2021 roku, sprawozdanie z działalności Najwyższej Izby Kontroli w 2021 roku oraz 175 informacji o wynikach kontroli planowych i doraźnych. Komisje sejmowe zgłosiły 78 sugestii kontroli i spośród 22 tematów zarekomendowanych przez Komisję do Spraw Kontroli Państwowej do planu pracy NIK na 2023 rok przyjęto 7. Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii zgłosiła nam jedną sugestię dotyczącą kontroli realizacji Narodowego Planu Szerokopasmowego. Zagadnienie to zostało ujęte w planie pracy NIK na 2023 rok i kontrola ta będzie realizowana od września tego roku. Obecnie jesteśmy na etapie opracowywania programu kontroli.

W rozdziale 2 sprawozdania przedstawiono realizację zadań państwa w świetle kontroli NIK. Działalność kontrolna NIK koncentrowała się na zagadnieniach istotnych z punktu widzenia obywatela, jak i państwa. Kontrole obejmowały problematykę szeroko rozumianego bezpieczeństwa obywateli państwa, jego rozwój gospodarczy, a także odpowiedzialność za środowisko. Jeżeli chodzi o wyniki kontroli będących w zainteresowaniu Wysokiej Komisji, to w okresie objętym sprawozdaniem NIK przeprowadziła kontrolę

z zakresu sieci komputerowych, informatyzacji oraz rozwoju społeczeństwa informacyjnego. W 2022 roku Departament Administracji Publicznej, który bezpośrednio reprezentuję, przeprowadził jedną kontrolę doraźną: „Efekty realizacji przez jednostki samorządu terytorialnego projektu w zakresie usług elektronicznych w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014–2020”. Informacja o wynikach kontroli została przekazana już do Sejmu. Kontrola ta wykazała nieprawidłowości w zapewnianiu obywatelom dostępności do tych e-usług w okresie trwałości projektów. Spośród łącznej liczby 206 e-usług przewidzianych do udostępnienia w ramach projektów w praktyce dostępne były tylko 172 usługi, czyli 83%, a 34 e-usługi były faktycznie niedostępne dla mieszkańców. W przypadku 64% e-usług uruchomionych w ramach zbadanych projektów zainteresowanie nimi było niewielkie lub nikt z nich nawet nie korzystał. Nie w pełni zatem osiągnięto zakładane zwiększenie dostępności e-usług i korzystania z nich.

Realizacja projektów przyczyniła się natomiast do wzmocnienia rozwiązań informatycznych w urzędach jednostek samorządu terytorialnego w obszarze usług elektronicznych. Stwierdzone jednak w urzędach jednostek samorządu terytorialnego nieprawidłowości polegały między innymi na zapewnieniu ciągłego dostępu do uruchomionych usług, niewykorzystaniu zakupionych w ramach projektów urządzeń, nieudostępnianiu aplikacji mobilnej dla mieszkańców czy zaprzestaniu korzystania z zakupionego w ramach projektu systemu elektronicznego zarządzania dokumentacją.

Kolejnym zagadnieniem w zakresie informatyzacji objętym kontrolą NIK była między innymi kontrola działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych z tym kradzieży tożsamości. Kontrola jest nadzorowana przez Departament Porządku i Bezpieczeństwa Wewnętrznego. Informacje o wynikach kontroli będzie państwu przedstawiona tutaj przez dyrektora departamentu w kolejnym punkcie porządku obrad Wysokiej Komisji. Ponadto NIK przeprowadziła również kontrole dotyczące: cyfryzacji ewidencji gruntów i budynków na szczeblu powiatowym, elektronicznych wniosków i tytułów wykonawczych w postępowaniu egzekucyjnym w administracji, bezpieczeństwa informacji w pracy na odległość i mobilnym przetwarzaniu danych, realizacji procesu informatyzacji w Agencji Restrukturyzacji i Modernizacji Rolnictwa, małopolskiego systemu informacji medycznej w latach 2016–2021 oraz realizacji projektu pod nazwą Konwersja Cyfrowa Domów Kultury w wybranych samorządowych jednostkach kultury województwa mazowieckiego. Dodatkowo NIK przeprowadziła jedną kontrolę doraźną w urzędzie miasta Poznania dotyczącą gospodarowania licencjami komputerowymi.

Większość wymienionych przeze mnie kontroli została zaprezentowana właściwym komisjom sejmowym lub podkomisjom. Jeżeli macie państwo jakieś pytania, pozostaję do dyspozycji. Dziękuję.

Przewodniczący poseł Grzegorz Napieralski (KO):

Chciałem pani dyrektor bardzo serdecznie podziękować za wyczerpującą informację i przedstawienie jej Komisji. Otwieram dyskusję. Czy są jakieś pytania do pani dyrektor bądź ktoś chce zabrać głos w tym punkcie? Nie widzę. W takim razie zamykam dyskusję. Pozostało nam jeszcze uchwalenie opinii dla Komisji do Spraw Kontroli Państwowej. Jeżeli nie usłyszę… Pan minister? Proszę.

Podsekretarz stanu w Ministerstwie Cyfryzacji Paweł Lewandowski:

Tutaj został przedstawiony raport, który chyba nie jest zgodny z…

Przewodniczący poseł Grzegorz Napieralski (KO):

Żeby wyjaśnić, bo również pan przewodniczący ma wątpliwości... W pierwszym punkcie mamy rozpatrzenie i zaopiniowanie dla Komisji do spraw Kontroli Państwowej Sprawozdania z działalności Najwyższej Izby Kontroli. A jak rozumiem, pana ministra pytanie dotyczy raczej drugiego punktu.

Podsekretarz stanu w MC Paweł Lewandowski:

OK... Został przedstawiony cały szereg różnych rzeczy, które pozostały jakby niezrealizowane lub nie do końca się wydarzyły. Przy czym z tego, co usłyszałem z raportu, gene-

ralnie większość tych spraw dotyczy nieodpowiedniego wykorzystywania usług przez samorządy. Niewdrożenie tych usług, niewykorzystanie sprzętu, nierealizowanie zadań przez samorządy w zakresie EZD. Dobrze usłyszałem?

Pełniąca obowiązki wicedyrektor Departamentu Administracji Publicznej NIK Agnieszka Bernaś-Coşkun:

Panie ministrze, przedstawiłam pokrótce jedną z kontroli, której wyniki przesłaliśmy już do Sejmu, natomiast jeszcze nie była ona przedmiotem obrad Wysokiej Komisji. Myślę, że w najbliższym czasie będzie. Dotyczyła ona wyłącznie e-usług w jednostkach samorządu terytorialnego. Dziękuję.

Podsekretarz stanu w MC Paweł Lewandowski:

Rozumiem. Dziękuję.

Przewodniczący poseł Grzegorz Napieralski (KO):

Tylko wyjaśnię, panie ministrze. Pani dyrektor przedstawiła tak naprawdę, jakie NIK ma zadania, które wykonała, które ma do wykonania. Pani dyrektor powiedziała, że jest wniosek naszej komisji dotyczący kontroli, który jest w przygotowaniu. Rozumiem, że przygotowywany jest plan. My mamy dzisiaj po wysłuchaniu, mamy stwierdzić, czy to, co pani dyrektor nam przedstawiła, przyjmujemy czy też opiniujemy negatywnie.

Pan przewodniczący Czarnecki.

Poseł Witold Czarnecki (PiS):

Panie przewodniczący, panie ministrze, jednak pierwsze zarzuty z pani strony były bardzo ogólnej natury. Nie dotyczyły samorządów, tylko dotyczyły jakichś niedociągnięć. Padały kwoty miliardów złotych. To z całą pewnością nie dotyczyło samorządu. Bo tu padały nawet – chyba że się pani przejęzyczyła – nawet setki miliardów. To są liczby straszne… Na pewno nie mogło dotyczyć to samorządu. Jedyna liczba, która mogła dotyczyć samorządów, to było 180 milionów. Rzeczywiście taka liczba może być do zaakceptowania, ale nie miliardy.

Pełniąca obowiązki wicedyrektor Departamentu Administracji Publicznej NIK Agnieszka Bernaś-Coşkun:

Przedstawiłam kwotę 20 mld zł jako wymierny skutek wszystkich kontroli Najwyższej Izby Kontroli w 2022. Nie wymieniłam tej kwoty w kontekście jednostek samorządu terytorialnego. Nie wymieniłam nawet żadnej kwoty w kontekście JST. Wszystko to są główne ogólne kwoty dotyczące wszystkich 180 tematów kontroli. Dziękuję.

Poseł Witold Czarnecki (PiS):

A czy mogłaby pani powiedzieć, jaka kwota przypadała na samorządy, a jaka na brak działań albo złe działania rządu?

Pełniąca obowiązki wicedyrektor Departamentu Administracji Publicznej NIK Agnieszka Bernaś-Coşkun:

Nie mamy takiego podziału tutaj.

Poseł Witold Czarnecki (PiS):

Wielka szkoda. Dziękuję bardzo.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję, panie przewodniczący, bardzo dziękuję, pani dyrektor. Czy są jeszcze głosy w dyskusji? Pan przewodniczący, bardzo proszę.

Poseł Witold Czarnecki (PiS):

Tak. Z uwagi na to, że nie dostaliśmy podstawowych odpowiedzi, proponuję zaopiniować negatywnie sprawozdanie NIK. Dziękuję bardzo.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję. W przypadku pojawienia się sprzeciwu, a taki sprzeciw się pojawił – przedstawił go pan przewodniczący Czarnecki – będziemy teraz głosować. Proszę się przygotować do głosowania. Kto z pań i panów posłów jest za negatywnym zaopiniowaniem sprawozdania z działalności Najwyższej Izby Kontroli?

Jeszcze raz. Kto z pań i panów posłów jest za negatywnym zaopiniowaniem sprawozdania z działalności Najwyższej Izby Kontroli za rok 2022? Kto jest przeciw? Kto się wstrzymał? Dziękuję bardzo.

Głosowało 15 osób. Za 9, przeciw 6, nikt się nie wstrzymał. Stwierdzam, że Komisja zaopiniowała negatywnie sprawozdanie z działalności Najwyższej Izby Kontroli w 2022 roku – tym samym uchwaliła opinię w tej sprawie, którą przekażemy do Komisji do Spraw Kontroli Państwowej. Bardzo dziękuję, pani dyrektor.

Przechodzimy do punktu drugiego porządku obrad. Proszę pana Tomasza Sordyla, pełniącego obowiązki dyrektora Departamentu Porządku i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli o przedstawienie informacji NIK o wynikach kontroli „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości".

Bardzo proszę pana ministra Pawła Lewandowskiego, podsekretarza stanu w Ministerstwie Cyfryzacji o przedstawienie stanowiska ministra do informacji NIK o wynikach kontroli. Poproszę również o zabranie głosu pana inspektora Michała Pudło, zastępcę komendanta Centralnego Biura Zwalczania Cyberprzestępczości o przedstawienie stanowiska komendanta głównego policji do informacji NIK o wynikach kontroli.

Pełniący obowiązki dyrektora Departamentu Porządku i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli Tomasz Sordyl:

Rozumiem, że my jako pierwsi. Szanowny panie przewodniczący, szanowni państwo, bardzo dziękujemy za zaproszenie na posiedzenie Komisji i możliwość przedstawienia naszego raportu.

Kontrola „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości" była kolejną kontrolą NIK dotyczącą obszaru cyberbezpieczeństwa. Od ponad 10 lat NIK bada te zagadnienia, w szczególności aspekt działania poszczególnych organów państwa, których zadaniem jest ochrona naszego wspólnego bezpieczeństwa. Obserwujemy, jak wiele zmieniło się na lepsze w tym czasie, również dzięki realizacji wniosków i rekomendacji Najwyższej Izby Kontroli.

Jeszcze 10 lat temu administracja państwowa ograniczała się w zasadzie do ochrony swoich własnych systemów. Poszczególne działania były realizowane w sposób rozproszony, a świadomość istniejących zagrożeń i wyzwań była pod tym względem na stosunkowo niskim poziomie. Szanowni państwo, wiele zmieniło się w naszym kraju na lepsze w kwestii cyberbezpieczeństwa, ale nie oznacza to, że obecnie funkcjonujący system odpowiada już na wszystkie wyzwania. Nadal pozostaje wiele do zrobienia, zwłaszcza, że metody działania i narzędzia wykorzystywane przez cyberprzestępców również ciągle się rozwijają. Zapewnienie bezpieczeństwa w cyberprzestrzeni stało się problemem społecznym i gospodarczym mającym bezpośredni wpływ na bezpieczeństwo państwa, gospodarki i wszystkich obywateli. Nie ukrywam, że właśnie ta perspektywa zwykłego obywatela tutaj znalazła mocny wyraz, w kontroli którą przeprowadziliśmy. Chcieliśmy spojrzeć właśnie przez pryzmat przeciętnego obywatela naszego kraju narażonego właśnie na różnego rodzaju formy cyberprzestępczości: jak wygląda jego ochrona, czy może znaleźć skuteczną pomoc, jeżeli stanie się już ofiarą przestępstwa, czy są prowadzone różnego rodzaju działania, które mają go uchronić przed tym, żeby nie stał się ofiarą tego przestępstwa.

Jeżeli pan przewodniczący pozwoli, to poproszę teraz pana głównego specjalistę Daniela Michaleckiego, żeby przedstawił bardziej szczegółowo wyniki tej kontroli, a później jeszcze króciutko podsumujemy. Dziękuję bardzo.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo. Proszę uprzejmie.

Główny specjalista kontroli państwowej w Departamencie Porządku i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli Daniel Michalecki:

Szanowny panie przewodniczący, Wysoka Komisjo, przeprowadzając tę kontrolę, wyszliśmy z założenia, że skoro państwo zaprasza obywateli do cyberprzestrzeni, w której działają urzędy, platformy, przez które można składać wnioski, w której można – a nawet

już w pewnych aspektach tylko tam – załatwić urzędową sprawę, to państwo powinno również wziąć odpowiedzialność za bezpieczeństwo tych obywateli w tym wirtualnym obszarze oraz aktywnie przeciwdziałać pojawiającym się zagrożeniom.

W tym miejscu podzielę się z państwem osobistą historią. Studiowałem kiedyś w szkole, która powstała na pofabrycznych terenach. Mówiąc krótko, była to warszawska Praga. To były początki tej szkoły. Żeby dojść od tramwaju do uczelni trzeba było przejść przez nieciekawą okolicę. To było 200–300 m, ale trzeba było przebrnąć przez takie różne kamienice. I niestety pojawił się problem polegający na tym, że studenci, którzy docierali na tę uczelnię, zaczęli być atakowani, rabowani. Oczywiście w tej sytuacji uczelnia mogłaby powiedzieć – to jest państwa problem, proszę sobie zapewnić bezpieczne dotarcie, my zapewniamy państwu bezpieczeństwo w murach tej szkoły. Ale uczelnia zainterweniowała w inny sposób. Po pierwsze rozpoczęła akcję edukacyjną skierowaną do studentów informującą o tych zagrożeniach, akcję edukacyjną, w ramach której zalecała chodzenie grupami przez ten niebezpieczny teren. Co więcej, zatrudniła firmy ochroniarskie, które stały w tych najważniejszych godzinach, w tym ciągu komunikacyjnym – między główną ulicą z tramwajem a uczelnią, żeby po prostu zapewnione było bezpieczeństwo tych studentów.

Przeprowadzając tę kontrolę, wyszliśmy właśnie z takiego założenia, że państwo powinno zareagować w podobny sposób, jak ta szkoła – aktywnie wychodzić z akcją edukacyjną do obywateli oraz zapewnić im bezpieczeństwo poprzez przeciwdziałanie różnym zagrożeniom. Jeszcze jedna uwaga. Też państwo znacie ze szkoły taką sytuację, kiedy nauczyciel zwraca się do uczniów z pretensją – czemu was jest tak mało? To dotyczy tych uczniów, których nie ma, a mówi do tych, którzy akurat są. Tak to jest z kontrolami naszej instytucji, że krytykujemy osoby, które siedzą obok, które są aktywnie zaangażowane w zapewnianie bezpieczeństwa. Chcę wyraźnie podkreślić, że doceniamy państwa wysiłek, państwa zaangażowanie, pracowników administracji, w tym Ministerstwa Cyfryzacji i funkcjonariuszy poszczególnych służb, w tym Policji, pracowników NASK, w zapewnienie Polakom bezpieczeństwa w cyberprzestrzeni. Nie możemy jednak pominąć milczeniem i musimy wskazać na obszary, które zgodnie z ustaleniami naszej kontroli wymagały i przynajmniej częściowo dalej wymagają poprawy.

Szanowni państwo, do kontroli wybraliśmy kluczowe podmioty realizujące zadania w zakresie zapobiegania i ograniczania skutków przestępstw internetowych – a więc wspomniane przed chwilą ministerstwo cyfryzacji, pełnomocnika rządu do spraw cyberbezpieczeństwa, komendanta głównego policji oraz dyrektora Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego.

Podstawowe pytanie, które nam towarzyszyło, brzmiało: czy organy państwowe prowadzą adekwatne działania w celu identyfikowania, zapobiegania oraz ograniczenia skutków przestępstw internetowych? Jedno ważne zastrzeżenie – kontrola dotyczyła wybranych przestępstw popełnianych w cyberprzestrzeni. Takich, które miały wymiar finansowy, narażały na straty finansowe osoby fizyczne, a więc kradzież tożsamości, która mogła do tego prowadzić, phishing. Nie zajmowaliśmy się mową nienawiści czy pedofilią w tej kontroli.

Skoncentrowaliśmy się na tym, czy indywidualni użytkownicy internetu są informowani na temat grożących im niebezpieczeństw, a w sytuacji, gdy staną się celem ataku, czy mogą liczyć na wsparcie właściwych instytucji państwowych. Kontrolę rozpoczęliśmy pod koniec 2021 roku, więc przyjęliśmy, że przyjrzymy się działaniom wskazanych wyżej podmiotów w okresie trzyletnim – od 2019 do 2021 roku.

Szanowni państwo, ogólna ocena kontrolowanej działalności – stwierdziliśmy, że w kontrolowanym przez nas okresie tworzony w Polsce system cyberbezpieczeństwa koncentrował się na wzmocnieniu bezpieczeństwa systemów uznawanych za kluczowe dla funkcjonowania państwa. I to dobrze. Jednak jego wadą było to, że pomijał on w praktyce najliczniejszą grupę użytkowników internetu, którymi są osoby fizyczne. A to źle. Tym bardziej że prowadzona analiza ryzyka oraz monitoring zagrożeń jednoznacznie wykazywały, iż dominującą i gwałtownie zwiększającą się kategorią incydentów w cyberprzestrzeni były oszustwa komputerowe, w tym phishing i kradzież tożsamości i wymierzony w indywidualnych użytkowników sieci. To, co nas zaniepokoiło to to, że w tym

badanym przez nas okresie organy odpowiedzialne za bezpieczeństwo cyberprzestrzeni oraz koordynację polityki rządu w tym obszarze – a więc minister cyfryzacji i pełnomocnik rządu do spraw cyberbezpieczeństwa – nie reagowali na te ryzyka oraz zagrożenia. Nie dostosowywali do nich swoich działań organizacyjnych i informacyjnych.

W ocenie tych organów cały obszar bezpieczeństwa obywateli w sieci oraz zagrożeń ze strony przestępczości internetowej pozostawał jakby poza ich odpowiedzialnością. Nie widzieli oni konieczności podejmowania w tym zakresie działań, wskazywali natomiast inne instytucje jako odpowiedzialne za ten obszar.

Krótko o wynikach kontroli, najważniejsze ustalenia. Wszystkie podmioty, które zbadaliśmy, prowadziły regularną analizę ryzyka, analizę zdarzeń, zagrożeń, incydentów występujących w internecie. Przykładowo pełnomocnik rządu do spraw cyberbezpieczeństwa od początku 2021 roku dostawał w układzie miesięcznym szczegółowe raporty z CSIRT NASK, w którym wskazywano na rodzaj i skalę zagrożeń w sieci. Wyniki raportów były jednoznaczne. Wskazywały, że w poszczególnych miesiącach do 90% zdarzeń to oszustwa komputerowe – phishing dotykający indywidualnych użytkowników internetu. Jednak podczas gdy Policja i NASK reagowały lub przynajmniej próbowały reagować na wyniki tych analiz, mówię tutaj o dostosowywaniu procedur działania, proponowaniu zmian strukturalnych, propozycjach zmian legislacyjnych, to w przypadku tych kluczowych organów dla krajowego systemu cyberbezpieczeństwa, a więc ministra cyfryzacji i pełnomocnika, którzy mieli koordynować, spajać cały krajowy system cyberbezpieczeństwa, takich skoordynowanych zaplanowanych działań nie dostrzegliśmy.

Pełnomocnik i minister konsekwentnie budowali system cyberbezpieczeństwa ukierunkowany na jego instytucjonalnych interesariuszy, np. operatorów usług kluczowych, dostawców usług internetowych, samorząd. Gdzieś w tym wszystkim naszym zdaniem gubił się jednak indywidualny użytkownik internetu. Obowiązujący podczas naszej kontroli dokument, jakim jest Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 wpisywała i wpisuje się przy tym w pewną niedobrą tradycję podobnych dokumentów w naszym kraju. Wszystkie te dokumenty cierpią na jeden problem – brak konkretów, co czyni z nich bardziej zbiór życzeń niż dokument, według którego podejmowane mogą być konkretne działania. Nawet jeśli więc ochrona indywidualnych obywateli była wpisana w strategię, to w kontrolowanym okresie nic lub bardzo niewiele z tego wynikało.

Niestety po raz kolejny nie będzie to dla państwa zaskoczeniem, ponieważ wskazaliśmy na bolączkę administracji publicznej, na jaką cierpi ona od wielu lat, czyli brak zasobów, brak specjalistów, w jakimś zakresie też sprzętu i oprogramowania. W przypadku Kancelarii Prezesa Rady Ministrów departament merytoryczny, który tak naprawdę powinien sterować, koordynować, sprawować pieczę nad całym systemem cyberbezpieczeństwa pod koniec naszej kontroli liczył 21 pracowników i borykał się z potężną fluktuacją kadrową. Ludzie pojawiali się tam i znikali po krótkim czasie. Z całą pewnością tak wąski zespół, pomimo zaangażowania i kompetencji, nie był w stanie podołać tym wszystkim zadaniom, których byśmy od niego oczekiwali. Była to zresztą opinia, którą wyraził sam minister i pełnomocnik rządu do spraw cyberbezpieczeństwa.

Te problemy kadrowe i sprzętowe dotykały również Policję. W kontrolowanym okresie nie miała ona wystarczającej liczby funkcjonariuszy, żeby zajmować się tematyką cyberbezpieczeństwa, a potrzeby sprzętowe czy software'owe przekraczały możliwości budżetowe tej formacji. Trzeba jednak zauważyć, że kierownictwo Policji dostrzegło ten problem i podjęło działania zaradcze. Pod koniec 2021 roku została powołana zupełnie nowa, wyspecjalizowana jednostka organizacyjna Policji – Centralne Biuro Zwalczania Cyberprzestępczości. Bardzo dobry, sensowny, zbieżny z naszymi przemyśleniami projekt. Podstawowe ryzyko, jakie mu towarzyszy polega na tym, że komendant główny policji założył, iż do końca 2025 roku uda mu się osiągnąć pełną operacyjność tej jednostki – to znaczy pozyskać prawie 2000 wysokiej klasy specjalistów. Znając specyfikę rynku IT i wysokość uposażeń na rynku IT może być to trudne. Ale na pewno policja powinna zrobić wszystko, by ta jednostka działała tak jak zostało to zaplanowane i zamierzone.

Szanowni państwo, kolejny problem to zgłaszanie przestępstw internetowych. Zidentyfikowaliśmy tutaj utrudnienia w zgłaszaniu tego rodzaju przestępstw przez obywateli.

W przypadku Policji, która dla zdecydowanej większości osób jest pierwszym miejscem, gdzie zgłaszane są tego typu zdarzenia, nie opracowano żadnych procedur i instrukcji dla obywatela, który pojawia się tam z takim specyficznym problemem. W przypadku funkcjonariuszy przyjmujących zgłoszenie wypracowano specjalne algorytmy działań. Miały one pomagać funkcjonariuszom, przede wszystkim tym nieposiadającym wiedzy specjalistycznej. To była zdecydowana większość. Pomysł bardzo dobry, jednak przy współpracy z naszym ekspertem zidentyfikowaliśmy mankamenty tych algorytmów. Po pierwsze nie były one aktualizowane. Po drugie mimo wszystko w naszej ocenie wymagały od policjantów wiedzy specjalistycznej. Dobre, precyzyjne procedury przyjmowania zgłoszeń na temat incydentów w sieci wypracowano po stronie NASK. Tu był jednak inny problem – z naszych badań sondażowych wynikało, że w kontrolowanym przez nas okresie tylko 1% obywateli tak naprawdę wiedział, co to jest NASK, czym się NASK zajmuje, że tam ewentualnie jest zespół CSIRT, który może świadczyć wsparcie dla osób fizycznych. Te ograniczenia powodowały, drodzy państwo, że obywatele często rezygnowali z zawiadamiania właściwych organów, że stali się celem ataku przestępców internetowych.

Przyjrzeliśmy się także temu, jak państwo poprzez swoje instytucje podnosi poziom kompetencji obywateli. Nasza ocena tych działań była ostatecznie negatywna. Oceniliśmy je jako nierzetelne i nieskuteczne. Dlaczego? Brak było jednolitego modelu informowania obywateli o zagrożeniach występujących w sieci. Zidentyfikowaliśmy tutaj sytuację, w której minister cyfryzacji od 2019 roku budował model, który my określiliśmy terminem modelu scentralizowanego. Model ten w ramach rządowego Portalu gov.pl tworzył bazę wiedzy z zakresu cyberbezpieczeństwa. W tej bazie zamieszczone są różnego rodzaju artykuły, ostrzeżenia, rekomendacje dla specjalistów, dla osób fizycznych. Tworzono repozytorium wiedzy, gdzie jako obywatele możemy szukać informacji o zagrożeniach i wskazówkach, jak mamy zachować się w sytuacji, która nas spotkała. Odmienną praktykę przyjął dyrektor NASK. Tworzył system, który my nazwaliśmy systemem rozproszonym – system różnych stron internetowych, portali. Problem polega jednak na tym, że NASK nadzorowany jest przez ministra cyfryzacji. Prosiło się w naszej ocenie, by szef tego procesu zdecydował, w którą stronę jako państwo idziemy – w stronę modelu centralnego czy rozproszonego.

Z kolei Policja docierała do obywateli poprzez informacje zawierane głównie w swoich aktualnościach. Działała prewencyjnie. Miały one charakter migawki, doraźnej informacji, która pojawiała się i znikała. Komendant główny zgodził się z nami, że trafionym pomysłem byłoby zbudowanie bazy wiedzy – trwałej, aktualizowanej, łatwo dostępnej, łatwo wyszukiwalnej. Stwierdził, że ten pomysł powinno zrealizować Centralne Biuro Zwalczania Cyberprzestępczości.

Jeśli chodzi o skuteczność działań edukacyjnych, to niestety nie miały one wysokiej skuteczności. Baza gov sprawiała wrażenie bazy ukrytej. Niewiele osób wiedziało o jej istnieniu. Natomiast analiza wyświetleń poszczególnych zakładek czy artykułów pokazywała, że te statystyki nie były oszałamiające – zarówno jeśli chodzi o ministerialną bazę wiedzy czy publikacje NASK, czy też Policji. Były oczywiście wyjątki, bo np. dany artykuł kliknęło 50 tys. osób, ale były to na przestrzeni tych 3 lat wyjątki. Przede wszystkim, proszę państwa, żaden z kontrolowanych przez nas podmiotów nie dokonywał oceny swoich publikacji pod kątem ich skuteczności w docieraniu i ich popularności.

Warto podkreślić ogromną aktywność NASK, mnóstwo publikacji, mnóstwo kampanii. Ale zabrakło prostego pytania: czy docieramy z tymi kampaniami, czy trafiamy? A jeśli nie, to co zrobić, żebyśmy dotarli, żebyśmy trafili do obywateli? I kolejna sprawa. Zazwyczaj te publikacje były niestety spóźnione, wobec tego co działo się akurat w danym okresie w cyberprzestrzeni.

Wybraliśmy w trakcie kontroli 6 dużych kampanii phishingowych z lat 2019–2021, pytając ministra i pełnomocnika, czy ostrzegał obywateli o tym, co im grozi. W przypadku czterech kampanii nie pokazano nam żadnych informacji zamieszczonych na stronach internetowych ministra. W przypadku dwóch luźno powiązane merytorycznie opracowania. I znowu wracamy do poprzedniego problemu: ile osób kliknęło w te artykuły, w te informacje, ile osób na nie oczekiwało? 300, czasami kilkadziesiąt. To nie jest ten efekt, którego byśmy oczekiwali.

Szanowni państwo, konkluzja – raczej przykra. W kontrolowanym przez nas okresie można było odnieść wrażenie, że państwo abdykowało w obszarze edukowania i ostrzegania obywateli o tym, co im może grozić i co im grozi w cyberprzestrzeni. Dużo skuteczniej działa w tym czasie sektor komercyjny, który potrafił dotrzeć z bezpośrednimi komunikatami do swoich klientów. W sytuacji, gdy byliśmy bombardowani fałszywymi wiadomościami od rzekomych firm kurierskich, rzekomych banków czy nawet rzekomych instytucji publicznych, jedynie prywatne firmy wysyłały skuteczne, bo docierające do użytkowników alerty.

Chcąc uzupełnić wyniki naszej kontroli, zleciliśmy podmiotowi zewnętrznemu sporządzenie sondażu opinii publicznej w kierunku tego, na ile obywatele czują się poinformowani o zagrożeniach w internecie i czy wiedzą, jak na nie reagować. Sondaż przeprowadzono zgodnie z zachowaniem wszystkich kanonów badań opinii publicznej na reprezentatywnej próbie tysiąca dorosłych osób. Bardzo nam zależało na tym i udało się tak przeprowadzić ten sondaż, że aż 404 osoby z tej grupy faktycznie zostały dotknięte atakami przestępców komputerowych. Zlecone przez NIK badanie sondażowe potwierdziło, że duża część spośród osób fizycznych nie wiedziała, co robić, ani gdzie się zgłosić w sytuacji ataku oszustów komputerowych. Ankietowani odpowiadali na przykład, że po skutecznie dokonanym na nich oszustwie internetowym nie zrobili nic, bo nie wiedzieli co mają zrobić. Nie zgłaszali spraw, bo nie wierzyli, że to coś da. Dlaczego nie wierzyli? Szanowni państwo, badanie tych 404 osób, które zostały dotknięte atakiem i zdecydowały się jednak zgłosić przestępstwo, wykazało, że tylko 2% spraw zakończyło się sukcesem, tj. wykryciem i skazaniem sprawcy lub odzyskaniem utraconych pieniędzy. Z kolei w przypadku 80% takich spraw ankietowani odpowiedzieli, że w sumie nie wiedzą, jak skończyło się postępowanie. Odpowiedzieli, że zakończyło się chyba niczym.

Szanowni państwo przyzwyczailiśmy się myśleć o bezpieczeństwie państwa i jego obywateli w tradycyjny sposób w wymiarze militarnym, bezpieczeństwa wewnętrznego, może zdrowia publicznego. Jednak w XXI wieku musimy dodać jeszcze jeden niezwykle ważny obszar bezpieczeństwa – cyberbezpieczeństwo. Obszar ten musi stać się jednym z priorytetów dla państwa polskiego, także jeśli chodzi o ochronę indywidualnych osób i dlatego po kontroli Izba przedstawiła następujące wnioski:

– po pierwsze, pierwsza grupa tych wniosków dotyczyła takich zmian w prawie i obowiązujących strategiach, by w większym zakresie uwzględniały one bezpieczeństwo indywidualnych użytkowników internetu;

– po drugie, postulowaliśmy o wdrożenie jednolitego modelu edukowania obywateli na temat bezpieczeństwa w sieci oraz stworzenie rozpoznawalnego, oficjalnego państwowego serwisu zawierającego łatwo dostępne informacje na temat zagrożeń cyberbezpieczeństwa, trwających kampanii, a także zaleceń i dobrych praktyk z zakresu cyberhigieny;

– po trzecie, wnioskowaliśmy o usprawnienie procesu przyjmowania zgłoszeń od obywateli i instytucji w sprawie przestępstw internetowych.

Szanowni państwo, na koniec musimy też przyznać, że w tym przypadku trafiliśmy na partnerów, którzy podjęli z nami dialog i podjęli konkretne działania w celu poprawy sytuacji. Jakie działania zostały podjęte po zakończeniu kontroli? Najważniejsze, które zasługują na podkreślenie, to przede wszystkim prace nad ustawą o zmianie niektórych ustaw w związku z zapobieganiem kradzieży tożsamości przewidującą między innymi możliwość skutecznego blokowania zaciągania zobowiązań; prace nad ustawą o zwalczaniu nadużyć w komunikacji elektronicznej – w jej ramach blokada wyłudzających wiadomości SMS oraz połączeń telefonicznych fałszujących numer abonenta.

Kolejna sprawa – działania podejmowane w celu popularyzacji S46. To był poboczny wątek naszej kontroli, ale ze względu na nakłady, jakie zostały poniesione na ten system, włączyliśmy go do naszego raportu. Deklaracja Komendy Głównej Policji o stworzeniu instrukcji postępowania dla ofiar cyberprzestępstw – instrukcji pomocnej przy zgłaszaniu przestępstw internetowych. Prace nad dostosowaniem narodowych standardów cyberbezpieczeństwa do krajowych realiów. Kampanie edukacyjne, które zaczęły być wreszcie widoczne. Na przykład kampania zachęcająca do weryfikacji dwuetapowej. Wreszcie na koniec doceniamy zwrot w myśleniu ministra i pełnomocnika o odpowiedzialności za

bezpieczeństwo osób fizycznych. Mam tu na myśli różne deklaracje, które przedstawiciele Ministerstwa Cyfryzacji wygłaszali chociażby na niedawnej konferencji CyberGOV.

Szanowni państwo, bardzo słusznie, oceniamy to bardzo pozytywnie. Bo na dobrą sprawę czy można skutecznie chronić instytucje, nie chroniąc indywidualnych użytkowników? Oni w tych instytucjach pracują. Ich słabość staje się słabością tych instytucji. A ich siła, świadomość, kompetencja chroni i wzmacnia te instytucje. Nie będzie bezpiecznej cyberprzestrzeni bez zapewnienia bezpieczeństwa indywidualnym użytkownikom internetu. Dziękujemy za uwagę.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo serdecznie dziękuję za bardzo szczegółową informację i wyjaśnienie wszystkich kwestii. Bardzo proszę teraz o zabranie głosu pana ministra Pawła Lewandowskiego, podsekretarza stanu w Ministerstwie Cyfryzacji. Bardzo proszę.

Podsekretarz stanu w MC Paweł Lewandowski:

Dziękuję bardzo. Panie przewodniczący, Wysoka Komisjo, przede wszystkim podkreślenia wymaga fakt, że ta kontrola dotyczyła sytuacji sprzed 2 lat. Oceniała 2 lata, sprzed 2 lat. To jest pierwsza kwestia, którą warto w tym miejscu podnieść. Stan cyberbezpieczeństwa osób fizycznych, czyli indywidualnych podmiotów w Polsce był pokłosiem tego, że od początku istnienia internetu panowała w nim zasada safe harbour, która polegała na tym, że nie robiono żadnych regulacji i to była ogólnie funkcjonująca na świecie polityka, i ktokolwiek jakąkolwiek zmianę chciał w tym zakresie zastosować, od razu był posądzany o cenzurę, regulowanie wolności słowa, i tak dalej. W związku z tym, że poziom cyberzagrożeń dramatycznie zaczął rosnąć w ostatnich latach – i to nie umknęło ani ministrowi cyfryzacji, ani pełnomocnikowi do spraw cyberbezpieczeństwa – zadania z tego zakresu dostały bardzo wysoki priorytet i między innymi dlatego w ogóle powołano w Polsce stanowisko pełnomocnika rządu do spraw cyberbezpieczeństwa.

W tym raporcie było pewne pomieszanie z poplątaniem. Przypisywano ministrowi cyfryzacji, czy też pełnomocnikowi rządu do spraw cyberbezpieczeństwa funkcje właściwe służbom, a nie centralnemu organowi administracji państwowej, który zajmuje się koordynacją i policy-makingiem. W zakresie wykonywania tych zadań tj. w zakresie policy-makingu i koordynacji zadań, w mojej ocenie i minister cyfryzacji, i pełnomocnik rządu do spraw cyberbezpieczeństwa wykonywali wszystkie zadania, które leżały w ich kompetencjach, a nawet te, które daleko wykraczały również poza te kwestie.

Jeden z zarzutów brzmiał, że pełnomocnik rządu do spraw cyberbezpieczeństwa zażyczył sobie comiesięcznych raportów, żeby wiedzieć, jaka jest skala problemu w sieci i że nic z tym nie zrobił. No właśnie, kiedy poprosił o te raporty i zidentyfikowano, jakie są tendencje, to wtedy została przygotowana cała strategia, która dotyczyła kwestii, które – tak jak powiedziałem – w tamtym czasie wykraczały poza kompetencje pełnomocnika rządu do spraw cyberbezpieczeństwa. A to dlatego, że tenże pełnomocnik został powołany do koordynacji cyberbezpieczeństwa na poziomie krajowym, a nie ścigania indywidualnych pospolitych przestępców, którzy po prostu nowe środki wykorzystywali do dokonywania tych samych przestępstw co zwykle, czyli: wyłudzeń, szantażów, okradania, podszywania się pod innych, kradzieży tożsamości. Te rzeczy się działy wcześniej, przed internetem i dzieją się teraz. Internet jest po prostu nowym polem, na którym te procedery się dzieją.

Największym problemem przy ściganiu tego typu przestępstw jest brak wykwalifikowanej kadry do tego. Osobom, które posiadają odpowiednie kompetencje, by zrozumieć istotę tych przestępstw i wiedzieć, jak je ścigać, na rynku pracy należy zapłacić bardzo dużo pieniędzy. Za każdym razem, kiedy państwo polskie chce w odpowiedni sposób wynagradzać urzędników, podnoszą się głosy, jakoby znowu państwo będzie tylko urzędnikom podnosić pensje, a zwykli ludzie nie będą mieli pieniędzy. A mimo to podnieśliśmy pensje osobom, które zajmują się cyberbezpieczeństwem. Powstała specjalna ustawa o wynagrodzeniach dla osób, które zajmują się tymi kwestiami. Kiedy minister Janusz Cieszyński został pełnomocnikiem rzeczywiście było tam zaledwie 20 osób, które się tym zajmowały i była olbrzymia rotacja. Ale dzisiaj mamy w pionie ministerstwa, który się zajmuje cyberbezpieczeństwem, 63 osoby bardzo wysoko wykwalifikowane, które mają

olbrzymie doświadczenie na rynku, w służbach i zajmują się tymi kwestiami w sposób bardzo systemowy.

Ponadto, tak jak tutaj raport zauważa na samym końcu – w momencie, kiedy zaczęto właśnie te raporty otrzymywać, pojawiły się ustawy, które zajmują się ochroną tożsamości, czy zastrzeganiem numeru PESEL. Jest procedowana ustawa dotycząca działań antysmishingowych, antyphishingowych we współpracy z telekomami. Warto zauważyć, że w raporcie powiedziano, że indywidualni, komercyjni usługodawcy czy sprzedawcy zajmowali się kształceniem swoich klientów pod kątem świadomości zagrożeń cyberbezpieczeństwa. To nie było tak, że oni rano się obudzili i powiedzieli – dobra, będziemy to robić. To my właśnie i NASK – tutaj reprezentant NASK siedzi – zgłaszaliśmy to do tych podmiotów. To CSIRT KNF zgłaszał tym podmiotom – bo to w szczególności dotyczyło banków – formy zagrożeń i inicjował te zadania za pomocą właśnie tych podmiotów. Bo o wiele szybciej te podmioty dojdą do swoich własnych klientów niż my za pomocą naszych kampanii, które też masowo rozpoczęliśmy. Kiedy zaczynała się kontrola, my właśnie wtedy uruchamialiśmy kampanie dotyczące informowania Polaków o cyberbezpieczeństwie.

Równolegle Policja powołała odpowiednie biuro specjalnie do tego dedykowane, które zajmuje się swoją właściwością, czyli ściganiem tych osób. My zajmujemy się monitoringiem, policy-makingiem i ewentualnie wskazywaniem dużych, istotnych zagrożeń dla dużych grup, dla instytucji, zagrożeń, które są w związku z wojną hybrydową. Dlatego jestem zdziwiony tym raportem. Mam wrażenie, że w momencie, kiedy go pisano, nie czytano, jakie są zadania poszczególnych podmiotów, które w tym systemie cyberbezpieczeństwa funkcjonują.

Dodatkowo warto zauważyć, że wczoraj pracowaliśmy nad ustawą o krajowym systemie cyberbezpieczeństwa. Tam zostały zgłoszone poprawki, ale oczywiście nie doszliśmy do tego momentu, ponieważ jednak Komisja większością opozycji, która była na miejscu, postanowiła odrzucić tę ustawę. Tam były dodatkowe…

Przewodniczący poseł Grzegorz Napieralski (KO):

Nie, panie ministrze. Proszę nie manipulować…

Podsekretarz stanu w MC Paweł Lewandowski:

Faktycznie uniemożliwiliście procedowanie tego w tej kadencji…

Poseł Konrad Frysztak (KO):

Proszę być szczegółowym w tym, co pan mówi. Jest pan przedstawicielem polskiego rządu.

Podsekretarz stanu w MC Paweł Lewandowski:

Proszę mi nie przerywać. Ja słuchałem wszystkich.

Poseł Konrad Frysztak (KO):

Pan kłamie.

Podsekretarz stanu w MC Paweł Lewandowski:

Ja nie kłamię, proszę pana. Pan dobrze wie, jaki jest efekt waszego przesunięcia.

Panie przewodniczący, proszę o porządek…

Przewodniczący poseł Grzegorz Napieralski (KO):

Proszę o spokój. Będę dawał głos w dyskusji. Będziemy mogli się do tego odnieść.

Podsekretarz stanu w MC Paweł Lewandowski:

W tej ustawie chcieliśmy między innymi dodatkowo wynagradzać właśnie Policję dodatkowymi środkami, żeby policjanci mieli więcej pieniędzy na lepszych specjalistów z rynku, żeby oni mogli pracować w tym systemie. To jest jedna kwestia.

Cały szereg ustaw w ostatnim czasie wszedł… Proszę pamiętać, że ustawa nie powstaje z dnia na dzień. Ustawa musi być przekonsultowania z rynkiem. Musimy przeprowadzić cały proces legislacyjny, konsultacji społecznych i dopiero trafia do Sejmu. W Sejmie również odpowiedni proces się musi odbyć i dopiero ona wchodzi w życie. To nie są rzeczy, które można zrobić w jeden dzień. W związku z powyższym cały ten raport, który się

odnosi do sytuacji sprzed 2 lat, kiedy te działania były wdrażane… W tamtym okresie powoływano dopiero pełnomocnika, który funkcjonował w i koordynował cały zakres działań i również wprowadzał dyrektywy i rozporządzenia europejskie działające w tym zakresie. Cały ten proces zaczął się w tamtym momencie. Kontrola dotyczyła momentu, kiedy faktycznie nie tylko w Polsce, ale w całej Unii Europejskiej, w gruncie rzeczy na świecie, dopiero zaczęto formułować centralne polityki i tworzyć odpowiednie służby, które zajmują się tymi kwestiami w związku z rozwojem internetu. Bo do tego momentu w tymże rozwoju również doszliśmy… W związku z tym powiem szczerze, że negatywnie patrzę na ten raport. Jego głównym efektem jest nieprawdziwe i zmanipulowane pokazanie rzeczywistości, przypisanie różnym organom kompetencji, których nie miały i pominięcie absolutnie całego kontekstu funkcjonowania internetu, a także momentu, w którym faktyczne działania mogły dopiero się rozpocząć. Dziękuję bardzo.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo serdecznie dziękuję, panie ministrze. Jeszcze nie ma dyskusji, ale jako przewodniczący muszę się odnieść do tego, co pan powiedział.

Po pierwsze sam przed chwilą pan powiedział, że proces legislacyjny polega na przygotowaniu ustawy, wprowadzeniu jej do Sejmu, przedyskutowaniu, przepracowaniu tej ustawy w Sejmie i dopiero ona wchodzi w życie. Jeżeli pan uważa, że na przepracowanie tak ważnej ustawy, która składała się z trzech tomów, ma być tylko jeden dzień… Dostaliśmy na to jeden dzień. Wczoraj mieliśmy złożyć sprawozdanie do pani marszałek. To nie jest czas na przepracowanie. Nikt nie złożył wczoraj wniosku o odrzucenie tej ustawy, bo wszyscy, jak na tej sali siedzimy, wierzymy i wiemy, że to jest najważniejsza ustawa. Tylko ona jest tak istotna i tak ważna, że ona powinna być punkt po punkcie przez długi czas przepracowana, żeby nie popełnić żadnego błędu. Próbowaliście nas i mnie osobiście oskarżać, że jesteśmy pod wpływem jakichś lobbystów. Właśnie dlatego chcemy szczegółowo pracować nad tą ustawą, żeby nikt nie zarzucił nam, że będzie jakikolwiek błąd. Błąd na rzecz jakiegoś lobbysty czy jakiejś firmy, czy jakiegoś państwa, które chciałoby w tej ustawie brać udział.

Przy takich ustawach, przy takiej wadze, panie ministrze, naprawdę potrzeba czasu i skupienia. Proponowaliśmy wczoraj, żeby powołać podkomisję, żeby w mniejszym gronie z ekspertami, z izbami gospodarczymi, przedstawicielami firm zainteresowanych taką dyskusję w parlamencie odbyć. W końcu po to jest parlament, żeby dyskutować. Nie chcieliście tego. Zaproponowaliśmy rozwiązanie moim zdaniem bardzo pozytywne i bardzo dobre – wysłuchanie publiczne. Na czym to polega? Każdy, kto chce, przychodzi do polskiego parlamentu i dyskutuje na temat tej ustawy. Nikt nie zablokował tej ustawy, panie ministrze.

Zróbmy tak. Pan minister powiedział swoje, ja się odniosłem, za chwilę otworzymy dyskusję. Pan inspektor czeka ze swoją prezentacją. I wrócimy do dyskusji, panie ministrze.

Podsekretarz stanu w MC Paweł Lewandowski:

Ad vocem, panie przewodniczący.

Przewodniczący poseł Grzegorz Napieralski (KO):

To ad vocem, a potem pan inspektor.

Podsekretarz stanu w MC Paweł Lewandowski:

Dziękuję, panie przewodniczący. Wczoraj podczas posiedzenia Komisji, kiedy któryś z przedstawicieli strony społecznej zaczął tłumaczyć coś panom posłom i paniom posłankom, pan przewodniczący Grabiec wyraźnie powiedział – my doskonale znamy tę ustawę. To po pierwsze.

A po drugie strona społeczna też ją doskonale zna, dlatego że my nie bez tej strony społecznej tworzyliśmy tę ustawę. Poza tym w trakcie dyskusji, w czasie pierwszego czytania były absolutnie wszystkie podmioty i wypowiedziały się na temat tej ustawy. Powiedziały, co się im podoba, co się im nie podoba. W tym procesie legislacyjnym mogły być od początku do końca. Wszystkie strony zostały wysłuchane. Co więcej, ja powiedziałem, że niektóre rzeczy w trakcie prac Komisji mogą zostać oczywiście zmodyfikowane po tym,

jak strony się wypowiedziały. Ponieważ one mogą na każdym etapie pracować i mogły zgłaszać poprawki w trakcie procedowania. Wysłuchanie publiczne nic nie zmieni, bo ci sami ludzie przyjdą i dokładnie to samo powiedzą. Nic więcej. Dziękuję bardzo.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo. Myśli pan, panie ministrze, że w 4–5 godzin byśmy przepracowali całą ustawę? Dalibyśmy radę? Patrzę na posłów i posłanki Prawa i Sprawiedliwości. Proszę odpytać posłów, panie ministrze – tu, ich po kolei – czy oni znają tą ustawę i konkretne przepisy i do czego ta ustawa dąży.

Poseł Witold Czarnecki (PiS):

Nie jesteśmy w sądzie amerykańskim…

Poseł Fryderyk Kapinos (PiS):

Panie przewodniczący, czy to jest lekcja?

Przewodniczący poseł Grzegorz Napieralski (KO):

To zapytajmy. Panie pośle, ma pan wiedzę na temat tej ustawy? Możemy o niej porozmawiać? Ja bardzo chętnie. Pytanie, czy pan ma wiedzę na temat tak ważnej ustawy.

Poseł Fryderyk Kapinos (PiS):

Co panu przeszkadza w niej?

Przewodniczący poseł Grzegorz Napieralski (KO):

To jak ją procedujecie, panie pośle. Przyszliście w piątek wieczorem i przynieśliście ją do Sejmu, w poniedziałek zawiesiliście ją na stronach, a kazaliście nam skończyć pracę we wtorek.

Poseł Robert Gontarz (PiS):

Nie można było przełożyć o miesiąc, a nie o 2 miesiące – w taki sposób, żeby to nie mogło wejść w życie?

Gdybyście naprawdę chcieli ją procedować, to złożylibyście wysłuchanie publiczne na przykład na za 2 tygodnie. Bo minimalny termin to są 2 tygodnie. Moglibyśmy przygotować wysłuchanie publiczne, ono by się odbyło i po tym wysłuchaniu publicznym moglibyśmy tę ustawę doprowadzić do końca. Jeśli wzięliście to na 11 września, to cała procedura potrwa tyle, że się zakończy po wyborach. Zatem to jest niemożliwe. Wy de facto złożyliście i przegłosowaliście wniosek o odrzucenie tej ustawy. Oczywiście nieformalnie, bo wy jesteście wielkimi demokratami. Ale w praktyce wy tę ustawę odrzuciliście. Ustawę, której nie chcą dwa państwa, wrogie Polsce, z wrogimi wywiadami. Pan doskonale wie, jakie to są państwa. Wy de facto tę bardzo ważną ustawę odrzuciliście. Jeśli wam się nie podobało procedowanie, można było o 2 tygodnie przełożyć to wysłuchanie. Na 2 tygodnie, na miesiąc, ale nie na 2 miesiące. Odrzuciliście tę ustawę tak naprawdę.

Przewodniczący poseł Grzegorz Napieralski (KO):

Panie pośle, powiem panu tak, pierwszy wniosek formalny, który padł z naszej strony zgłoszony przez pana posła Grabarczyka był taki, aby powołać podkomisję.

Podsekretarz stanu w MC Paweł Lewandowski:

Było głosowanie?

Przewodniczący poseł Grzegorz Napieralski (KO):

Drugi wniosek, który proponowaliśmy, żeby poszerzyć dyskusję nad tą ustawą o Komisję Administracji i Spraw Wewnętrznych, ponieważ kluczową była tak naprawdę kwestia dotycząca Policji. Też nie chcieliście tego. W rozmowie z panem ministrem i z przewodniczącym Jachem… Nie chcieliście żadnej z tych kwestii. Zaproponowaliśmy bardzo dobre rozwiązanie, które nazywa się wysłuchanie publiczne.

Poseł Witold Czarnecki (PiS):

Wniosek formalny.

Przewodniczący poseł Grzegorz Napieralski (KO):

Pan przewodniczący Czarnecki i pan poseł Konrad Frysztak. Bardzo proszę.

Poseł Witold Czarnecki (PiS):

Zgłaszam wniosek formalny, żeby wrócić do porządku obrad.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo. Jeszcze poseł Frysztak i wracamy…

Poseł Konrad Frysztak (KO):

Rezygnuję.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo, panie pośle. Panie inspektorze, oddaję panu głos. Musiał pan posłuchać trochę polityki. Przepraszam bardzo. Oddaję głos.

Zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości Komendy Głównej Policji insp. Michał Pudło:

Bardzo dziękuję. Szanowny panie przewodniczący, szanowni państwo, bardzo dziękuję za możliwość zabrania głosu.

Jest to dla mnie ciekawe doświadczenie uczestniczyć w takim przedsięwzięciu i posłuchać również polityki. Na wstępie chciałem bardzo podziękować kontrolującym z instytucji, która swój raport przedstawiała – został zauważony wysiłek Policji jaki został poniesiony, m.in. w celu zmniejszenia przestępczości – nazwijmy ją cyberprzestępczością – zmniejszenia przestępczości internetowej i w chronieniu obywatela przed tego rodzaju zagrożeniami.

Do tego, że te zagrożenia wzrastają lawinowo, nie muszę nikogo przekonywać, To jest sprawa oczywista. Natomiast sam raport porusza kilka kwestii, dotyczy instytucji, służby, którą reprezentuję, i przede wszystkim utrudnień, przede wszystkim wzmocnienia struktur etatowych, struktur organizacyjnych Policji jako tej instytucji, która ma zwalczać między innymi cyberprzestępczość. Dziękuję za to, że został zauważony proces powstawania Centralnego Biura Zwalczania Cyberprzestępczości – nowej jednostki Policji, którą mam przyjemność reprezentować. Biuro powstało dzięki państwu, dzięki ustawie z grudnia 2021 roku, która przewiduje powstanie nowej jednostki organizacyjnej Policji, która troszeczkę na wzór Centralnego Biura Śledczego Policji będzie zwalczała cyberprzestępczość. Ustawa przewiduje na 2025 rok 1800 etatów policyjnych specjalistów zwalczających tego rodzaju przestępczość. Oczywiście z każdym rokiem pomiędzy 2022 a 2025 ta liczba się zwiększa.

Ponadto raport mówi o utrudnieniu w dostępie obywatela do zgłaszania tego rodzaju przestępczości i braku procedur, braku algorytmów, które mogłyby pomagać w zgłoszeniu tego rodzaju przestępstw. Tutaj również Komenda Główna Policji i my jako Centralne Biuro Zwalczania Cyberprzestępczości pracujemy nad tym, aby faktycznie algorytmy były i umożliwiały obywatelowi złożenie zawiadomienia o przestępstwie czy uzyskanie pomocy, ale także pomagały funkcjonariuszom Policji w prawidłowym przyjęciu tego rodzaju zgłoszenia. To jest tytaniczna praca związana z tym, aby policjantów w terenie, również w najmniejszych komórkach organizacyjnych Policji, przeszkolić, aby posiadali taką wiedzę i umiejętności, które by to umożliwiały. To oczywiście jest zadanie dla Centralnego Biura Zwalczania Cyberprzestępczości i to realizujemy. W zeszłym roku ponad 1000 policjantów, mimo funkcjonowania CBZC od w zasadzie połowy roku… Na dobrą sprawę – tak kolokwialnie powiem – obchodzimy dziś rocznicę. 12 lipca w struktury CBZC wcielono pierwszych funkcjonariuszy, którzy prowadzili postępowania przygotowawcze. W ciągu zeszłego roku przeszkoliliśmy ponad 1000 policjantów. Dzisiaj już, do połowy roku, jest przeszło 1500 policjantów, którzy potrafią przyjąć zawiadomienie o przestępstwie w sposób taki, aby ułatwić prowadzenie postępowania przygotowawczego.

Raport porusza również kwestie pewnego ryzyka związanego z powstaniem tej nowej jednostki organizacyjnej Policji, czyli Centralnego Biura Zwalczania Cyberprzestępczości. To dzisiaj zostało już poruszone, czyli brak wykwalifikowanych specjalistów, którzy mogliby w tym biurze służyć. Oczywiście zdajemy sobie sprawę z tego ryzyka i robimy

wszystko, aby je zminimalizować. Na dziś biuro posiada 800 etatów. Aktualnie pełni służbę w naszym biurze 495 funkcjonariuszy, 450 jest na etatach. Były różne etapy rekrutacji. Pierwszy z etapów zakładał rekrutowanie policjantów, którzy wcześniej, przed powstaniem biura, zajmowali się zwalczaniem cyberprzestępczości, ale byli w strukturach komend wojewódzkich policji i komend miejskich, i powiatowych policji. To był pierwszy etap. Drugi etap był dla funkcjonariuszy Policji pełniących służbę w innych dziedzinach. A ponadto w tym roku trwa już pierwszy nabór kandydatów z cywila, czyli dla młodych ludzi. Przepraszam, nie tylko młodych. Ale dla ludzi, którzy chcieliby pełnić służbę w Policji i stać się funkcjonariuszami Policji zwalczającymi cyberprzestępczość. Wszystkie trzy sposoby rekrutacji się przeplatają. W pierwszych kilku miesiącach tego roku aplikację do CBZC z cywila złożyło około 250 osób. Myślę, że odniosłem się do wszystkich zagadnień związanych z poruszanymi kwestiami w raporcie, dotyczącymi Policji.

Mogę tylko powiedzieć na podsumowanie mojej wypowiedzi, że biuro jest w trakcie rozwoju. Robimy wszystko, aby werbować i być atrakcyjnym dla ludzi posiadających pewne umiejętności i kwalifikacje na rynku cywilnym. Także wśród policjantów. To też musi przebiegać w sposób dość łagodny, bo oczywiście nie możemy narazić innych komórek organizacyjnych policji na to, aby wszystkich ludzi stamtąd zabrać natychmiast. To wiązałoby się z pewnym ryzykiem dla wykonywania podstawowych zadań Policji. Na pewno nie narazimy Policji na takie ryzyko. To trwa.

Bardzo dziękuję. Oczywiście jestem do dyspozycji w przypadku jakichś pytań. Bardzo dziękuję, panie przewodniczący, za możliwość zabrania głosu.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję, panie inspektorze. Ja w dyskusji mam jedną propozycję, jedno pytanie, ale też propozycję dla Policji w sprawie współpracy z podkomisją.

Przedstawiciel CERT, bardzo proszę teraz pana Sebastiana Kondraszuka o zabranie głosu. Potem otwieram dyskusję.

Kierownik Działu CERT Polska w Naukowej i Akademickiej Sieci Komputerowej Sebastian Kondraszuk:

Panie przewodniczący, Szanowna Komisjo, szanowni państwo, CERT Polska od roku 1996 działa na rzecz przeciwdziałania problemom cyberbezpieczeństwa w sieci.

Nie będę tutaj przynudzał historią. W każdym razie my swoją działalnością staramy się pokazywać to, że jesteśmy na bieżąco z tymi problemami. Staramy się znaleźć na nie przede wszystkim receptę i w myśl współpracy systemowej starać się przedstawić skuteczne metody przeciwdziałania. Tematyka kontroli, w ramach której tutaj się spotykamy, niewątpliwie jest jednym z większym zagadnień problemowych, które leży oczywiście w polu operowania zespołu CERT Polska. Mowa oczywiście o przestępstwach popełnianych w sieci, przestępstwach, które prowadzą do kradzieży tożsamości obywateli. Sporym nadużyciem byłoby powiedzenie tutaj, że CERT Polska, realizując obowiązki krajowego zespołu cyberbezpieczeństwa, czyli CSIRT NASK, nie wywiązuje się lub wywiązuje się w sposób niewystarczający. Taki zarzut zawsze przy takiej skali szkodliwych działań można wysnuć. Natomiast na naszą obronę przytoczę kilka faktów.

Na przestrzeni kontrolowanego okresu przyjęliśmy 29 tys. zgłoszeń w roku 2019, 34 tys. zgłoszeń w roku 2020 i 65 tys. zgłoszeń w roku 2021, z czego większość pochodziła właśnie od osób indywidualnych. Jak kontrolujący zauważyli, w przytłaczającej części dotyczyło to przestępstw, bądź też prób wyłudzeń poufnych danych obywateli. W momencie rozpoczęcia pandemii zawiązał się w CERT Polska zespół – oczywiście możliwie blisko współpracujący z Departamentem Cyberbezpieczeństwa w Ministerstwie Cyfryzacji – który miał na celu w sposób predykcyjny przewidzieć, jakie będą konsekwencje takiego raptownego przejścia w tryb pracy zdalnej, a także tego, że mnóstwo procesów codziennych zostało w sposób może nie do końca kontrolowany przeniesione do przestrzeni internetu. Oczywiście to też wytworzyło pewnego rodzaju okazję dla cyberprzestępczości, która oczywiście skwapliwie z tego skorzystała.

Wiedzieliśmy, że będą rosły przestępstwa tego typu. Dlatego wyszliśmy z propozycją ustanowienia listy ostrzeżeń przed domenami wyłudzającymi dane internautów.

Przeważnie tutaj chodzi o ochronę osób fizycznych. To zadziało się w marcu 2020 r. Szanowni państwo, do dzisiaj na tej liście ostrzeżeń mamy już ponad 150 tys. wpisów. Nasi operatorzy w trybie ciągłym dokonują oceny i klasyfikacji tych domen. Wpisują domeny na listę ostrzeżeń. Natomiast działając w porozumieniu z operatorami telekomunikacyjnymi szkodliwa treść, która jest wyświetlana za pośrednictwem tych domen oznaczonych jako wyłudzające, jest blokowana dla użytkownika końcowego. W roku 2022 nasza lista z takich pobieżnych szacunków zadziałała blisko 21 milionów razy. Ta liczba naprawdę porażająca. Zaznaczam, że oczywiście nie każde z tych wywołań, sięgnięcia po naszą listę, czyli tych 21 milionów razy, to był obywatel zwiedziony przez tego atakującego, natomiast w bardzo dużej części. Jeżeli nawet założymy sobie, że co trzecia próba to była próba obrony tego oszukanego, to mówimy tutaj o bardzo dużej skali ochrony obywateli indywidualnych. W tym roku tych zgłoszeń kierowanych do CERT Polska będzie jeszcze więcej. Możemy oczywiście się spierać, czy jest to efekt tego, że postępuje cyfryzacja, czy jest to efekt popularyzacji cyberbezpieczeństwa, czy też prowadzonej kampanii w przestrzeni medialnej. Tego nigdy nie rozstrzygniemy, natomiast tych zgłoszeń w tym roku znowu będzie jeszcze więcej i zapewniam wszystkich państwa tutaj obecnych, że żadnego z nich nie pozostawimy bez odpowiedzi. Dziękuję.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo serdecznie dziękuję za tę informację. Otwieram dyskusję. Czy ktoś chciałby zabrać głos? Bardzo proszę, panie pośle.

Poseł Fryderyk Kapinos (PiS):

Chciałem bardzo serdecznie podziękować za pracę ministerstwu i wszystkim instytucjom.

Zorganizowałem też takie spotkanie z przedsiębiorcami... Przyjechał pan minister Cieszyński, przyjechali przedstawiciele NASK, ale również wojewódzkiej i powiatowej policji. Każdy z przedsiębiorców – mikro-, małych, średnich, dużych – mógł zadać pytanie, mógł taką informację od państwa uzyskać. Ja chciałbym, żeby tutaj z Policji to wybrzmiało, że obywatel może pójść na policję, do powiatu czy do dzielnicowego, czy do komendy wojewódzkiej i uzyskać taką informację na temat cyberbezpieczeństwa, jeżeli coś się stanie, jeżeli jest jakieś zagrożenie. Bardzo bym prosił, żeby to tutaj też wybrzmiało.

Druga sprawa dotyczy ustawy, którą wywołał pan przewodniczący. Chciałbym przeczytać tylko… Raport z opiniowania i konsultacji publicznych – chodzi o ustawę o cyberbezpieczeństwie – projekt ustawy o zmianie ustawy był konsultowany w ramach konsultacji publicznych. Skierowano zaproszenie do przedstawienia stanowisk do 51 podmiotów z 14 dniowym terminem na przedstawienie stanowiska. Jednakże z uwagi na prośby ze strony partnerów społecznych minister cyfryzacji przedłużył czas na uwagi o kolejne 14 dni. Tym samym termin na przedstawienie stanowiska wynosił 28 dni. Nie będę czytał tych wszystkich instytucji, które składały uwagi. Konsultacje publiczne oraz opiniowanie odbyły się w terminie od 8 września do 6 października 2020 roku, przy czym przyjmowano także uwagi przesłane w późniejszym terminie – pod warunkiem zgłoszenia tego faktu opiekunowi merytorycznemu projektu. W procedurze opiniowania i konsultacji publicznych projektu ustawy wszystkim podmiotom umożliwiono zajęcie stanowiska w sprawie projektu, a także poddano analizie przedłożone przez te podmioty uwagi. W ramach konsultacji publicznych i opiniowania zgłoszono szereg uwag do projektu ustawy. W ramach konsultacji 548 uwag, a w ramach opiniowania 53 uwagi. Myślę, że po prostu konsultacje się odbyły. Dziękuję.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję, panie pośle. Wróciłbym, jeżeli można, do pana inspektora. Ponieważ czytam, szczególnie w ocenach, konkluzjach i wnioskach o kwestiach dotyczących algorytmu przyjmowania zgłoszeń. Jest do tego dużo zastrzeżeń.

Moim zdaniem mimo słów pana ministra to do końca aż tak się nie poprawiło, mimo że trochę czasu minęło. Moja propozycja jest, panie inspektorze, taka – ponieważ w podkomisji zajmujemy się kwestią dotyczącą algorytmów i będziemy mieli jutro rozmowę z ZUS na ten temat, bo tam też szeroko algorytmy są używane, chciałbym zaproponować,

żebyśmy za 2 tygodnie na posiedzeniu Sejmu, razem z panem lub z kimś, kogo Policja wskaże, mogli w podkomisji o tym podyskutować o tym, co możemy zrobić, żeby jednak ułatwić wam tę pracę. Bo faktycznie wy jesteście pierwszym miejscem, do którego ludzie przychodzą. To nie jest zarzut, ale to najlepiej nie działa, panie inspektorze – żeby była jasność.

Materia jest oczywiście bardzo skomplikowana. Tu też NIK mówi o odpowiednich szkoleniach dla Policji, dla tych, którzy przyjmowaliby takie zgłoszenia. Warto by się nad tym bardzo poważnie zastanowić – też patrzę na pana ministra – i poszukać dodatkowych funduszy. Bo tak jak powiedziałem, wy jesteście tym pierwszym kontaktem dla obywatela. Często jest tak niestety, że policjant – i ja nie mam absolutnie tego za złe, bo był szkolony do czegoś innego – rozkłada ręce. Nie umie pomóc, tak jak powinien. A wszyscy wiedzą, gdzie pomocy szukać. Zawsze jak ktoś nas okradł, pobił, uderzył, szło się z tym na Policję. Myślę, że warto o tym porozmawiać co do kwestii finansowych, organizacyjnych – to bardziej pan minister i Komisja Administracji i Spraw Wewnętrznych. Natomiast co do kwestii algorytmów, jeżeli byłaby taka zgoda z waszej strony, wyślemy takie zaproszenie. Ja bym takie specjalne posiedzenie podkomisji zorganizował i porozmawialibyśmy o tym. Tym bardziej że będziemy mieć doświadczenie po pojutrzejszym posiedzeniu podkomisji w sprawie ZUS. Jeżeli byłaby taka zgoda, panie inspektorze…

Zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości KGP insp. Michał Pudło:

Bardzo dziękuję, panie przewodniczący. Oczywiście tak, jak najbardziej.

Wszystko, co pozwoli nam na poprawienie, choćby m.in. tego zakresu, jest słuszne. Bardzo dziękuję za to zaproszenie już z góry. Procedury, algorytmy muszą być, naszym zdaniem, podwójnego rodzaju – dla obywatela, żeby wiedział gdzie ma iść, co może zrobić, gdzie się może udać. Oczywiście do każdej komórki organizacyjnej Policji w terenie – jak pan poseł powiedział – może przyjść i uzyska pomoc. To jest dla mnie wyznacznik, żeby właśnie tak było za każdym razem – żeby ta pomoc była jak najlepsza. Mówię o tych pierwszych algorytmach, czyli dla obywatela. To, co on powinien wiedzieć. One powinny być i będą upublicznione w taki sposób, żeby było łatwe dotarcie. Drugi aspekt to szkolenia dla naszych policjantów i procedury dla policjantów, które z wiadomych przyczyn nie mogą być upublicznione, bo byłyby wtedy nieskuteczne. Tak jak już wcześniej mówiłem, staramy się oczywiście szkolić policjantów i będziemy szkolić dalej policjantów i nie tylko naszych z Centralnego Biura Zwalczania Cyberprzestępczości, ale też, co już się dzieje w terenie, czyli szkolenie policjantów, tak aby zawiadomienie było przyjęte jak najlepiej. Zdaję sobie sprawę, że to będzie proces ciągły i będzie musiał ulegać zmianom. Nawet te procedury… Między innymi w raporcie zostało opisane, że one nie są aktualne. One muszą być i będą aktualizowane jak najczęściej, przy każdej nadarzającej się okazji. Bardzo dziękuję.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję, panie inspektorze, za tę deklarację. Co do szkoleń i finansowania to już bardziej Komisja Administracji i Spraw Wewnętrznych, ale co do pomocy od strony technicznej czy też zmiany prawa nasza Komisja i podkomisja są do państwa dyspozycji.

Jeżeli mogę odpowiedzieć, bo pan poseł oprócz tego, że odnosił się do kwestii tego raportu, odniósł się również do wczorajszej sytuacji. Chciałbym pana poinformować o dwóch kwestiach, panie pośle.

Po pierwsze trzeba też mieć szacunek do parlamentu i do Sejmu, a szczególnie posłów i posłanek. Jak się wnosi bardzo poważną ustawę – to jest bardzo poważna ustawa – też trzeba dać nam czas, żeby się do niej przygotować i dać nam czas na dyskusję. Tak w polskim parlamencie było zawsze – przypominam panu – i powinno tak być. To jest pierwsza rzecz.

Druga rzecz, panie pośle. Dopominaliśmy się jako Komisja – być może pan nie był w naszej Komisji od samego początku – w tej kadencji o tę ustawę już bardzo dawno, żeby ją jak najszybciej wnieść i jak najwcześniej na spokojnie procedować.

Po trzecie taką ciekawostkę panu przeczytam, żeby pan wiedział, w jakiej my dzisiaj rzeczywistości żyjemy. Otóż z zgodnie z uzasadnieniem projektu ustawy, on ma imple-

mentować dyrektywę NIS. Tymczasem została przygotowana dyrektywa NIS2, która wejdzie niebawem w życie. Tak naprawdę już przepisy tej dyrektywy NIS2 powinny być implementowane, bo one wejdą za kilka miesięcy. To jest takie pokazanie w jakim systemie tak naprawdę pracujemy. Proszę nam nie zarzucać, że my coś robimy złego. Też proszę nas szanować i proszę nas traktować bardzo poważnie, również jako opozycję.

Tak samo było z ustawą o małoletnich. Mówiliśmy wam, że ustawę trzeba dobrze przygotować, a wy wrzuciliście do ustawy o małoletnich, jedną trzecią przepisów absolutnie z innych sfer. To jest poważne traktowanie naszej Komisji, posłów i posłanek? To nie jest, panie pośle, poważne taktowanie. Dlatego my się na taką pracę nie zgadzamy. Przed chwilą pan przewodniczący Czarnecki powiedział mi – na ucho, bo na ucho, ale mogę powtórzyć – od samego początku kadencji w naszej komisji jest najmniej sporów i najwięcej merytorycznej dyskusji. Chciałbym, żeby tak zostało. Bo naprawdę zajmujemy się… Tutaj nie ma fajerwerków, to prawda. Ale pracujemy nad ważnymi kwestiami. Do tej pory nie zdarzało się tak… Mogę użyć nawet takiego sformułowania – ja się czułem gwałcony. „Ma być tu i teraz, szybko, za 3 godziny”. No nie. Nie będzie tak, panie pośle.

Pan minister i pan przewodniczący. Proszę bardzo.

Podsekretarz stanu w MC Paweł Lewandowski:

W kwestii merytorycznej dotyczącej implementacji tejże dyrektywy – otóż ja tłumaczyłem na wczorajszym posiedzeniu, że my jesteśmy zobligowani do wdrożenia dyrektywy NIS w całości, niezależnie od tego, czy się pojawiają nowe przepisy czy nie. Te przepisy obowiązują do października przyszłego roku. W czasie, kiedy one nie obowiązują jest luka prawna. Poza tym możemy być narażeni na płacenie kar. Dodatkowo przepisy, które mają wejść w przyszłości, jakoś się diametralnie od tych przepisów nie będą różniły. One będą miały trochę szerszy zakres. I tak trzeba takie przepisy zrobić i jest niewiele do nowelizowania. Zatem ten argument jest absolutnie chybiony.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo, panie ministrze. Pan przewodniczący Czarnecki.

Poseł Witold Czarnecki (PiS):

Panie przewodniczący, Wysoka Komisjo, powiedzieć można wszystko. Jeżeli byłaby ze strony opozycji dobra wola, to oczywiście nad ustawą byśmy pracowali. Co do tego nie mam żadnych wątpliwości, ale był pewien plan polityczny. Ustalenie nawet daty – 11–12 września – pokazuje, że to była realizacja planu politycznego szkodzącego Polsce. A racjonalizować i tłumaczyć możemy wszystko. Dziękuję bardzo.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo, panie przewodniczący. Chciałem tylko dodać, że nie ma posiedzenia Sejmu w sierpniu. Jest po prostu wolne, więc nie możemy nic zorganizować w Sejmie. Nie ma w ogóle żadnego posiedzenia Sejmu.

Poseł Fryderyk Kapinos (PiS):

Panie przewodniczący, 28 sierpnia jest posiedzenie Sejmu…

Przewodniczący poseł Grzegorz Napieralski (KO):

A gdzie tak jest napisane?

Poseł Fryderyk Kapinos (PiS):

28 lipca.

Przewodniczący poseł Grzegorz Napieralski (KO):

A ja mówię o sierpniu, nie o lipcu.

Poseł Fryderyk Kapinos (PiS):

W sierpniu też będzie. Chcę powiedzieć, że wszyscy szanujemy każdego człowieka i nie może mi pan zarzucać, że tutaj nie ma jakiegoś szacunku do drugiego człowieka. Bo pan to zarzucił. Absolutnie tak nie jest.

Ja tylko przeczytałem z uzasadnienia, że te konsultacje się odbyły, a państwo mówiliście, że się nie odbyły. Odbyły się konsultacje z wieloma organizacjami. Wpłynęły wnio-

ski, wpłynęły uwagi. To zostało przeprocedowane w 2020 roku. 3 lata temu. Państwo też, jeżeli jesteście tacy bardzo wspaniali, mogliście się też włączyć, mogliście też poczytać. Mogliście uczestniczyć na tym etapie, nikt wam nie bronił.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję. Czy są głosy w dyskusji? Nie widzę. Jeszcze pan dyrektor. Bardzo proszę. I pani Joanna. Bardzo przepraszam. Pan dyrektor i pani Joanna, bardzo proszę.

Pełniący obowiązki dyrektora Departamentu Porządku i Bezpieczeństwa Wewnętrznego NIK Tomasz Sordyl:

Dziękuję bardzo. Panie przewodniczący, szanowni państwo, jeżeli państwo pozwolą bardzo króciutko jeszcze odniosę się do wypowiedzi pana ministra – bo tutaj chyba doszło do pewnej nieścisłości, którą chciałbym doprecyzować.

Pan minister podniósł, że Najwyższa Izba Kontroli pomieszała – chyba takie słowo zostało użyte – jeżeli chodzi o zakres obowiązków i przypisała ministerstwu zadania, które powinny być wykonywane przez służby, w tym Policję. Tutaj chciałem bardzo wyraźnie podkreślić, że w trakcie całej kontroli bardzo precyzyjnie odnosiliśmy się do zakresu działania poszczególnych podmiotów, również Ministerstwa Cyfryzacji i pełnomocnika rządu do spraw cyberbezpieczeństwa. Nawet wystąpił taki problem – wtedy jeszcze wszystko to było w Kancelarii Prezesa Rady Ministrów – że samo ministerstwo nie było w stanie wskazać, które zadania były realizowane przez ministra cyfryzacji, którym wówczas był pan premier Mateusz Morawiecki, a które były realizowane przez pełnomocnika rządu do spraw cyberbezpieczeństwa. To było też dość istotnym problemem z punktu widzenia realizacji kontroli. Oczywiście jest tak, że każdy obszar, który pojawia się zakresie działania organów państwa – a takimi niewątpliwie są kwestie cyberbezpieczeństwa – rodzi pewne problemy, również problemy o charakterze interpretacyjnym, jaki powinien być zakres działania i ingerencji państwa, w tym w tym obszarze.

My tutaj się odwołaliśmy na początku do kontroli sprzed 10 lat – jedna z pierwszych naszych kontroli. Takie stanowisko było nam prezentowane, że w zasadzie państwo nie ma żadnych zadań w zakresie cyberbezpieczeństwa. To się zmieniało na przestrzeni lat. Cieszę się – bo to wynika też z wypowiedzi samego pana ministra, również z deklaracji pana ministra Cieszyńskiego choćby właśnie na przywołanej tutaj wcześniej konferencji – że po naszej kontroli nastąpiła pewna zmiana i ministerstwo uznaje dzisiaj swoje zadania w zakresie zapewnienia bezpieczeństwa również obywatelom, a nie tylko instytucjom jako takim.

Drugą rzeczą, którą chciałem podkreślić, jest fakt, że jeżeli patrzymy na kontrolę, to zawsze musimy pamiętać, że kontrola jest na określony czas. Ona obejmuje jakiś czas, który został objęty właśnie tą kontrolą – 2, 3 lata z reguły. Jest jakiś stan na dzień zakończenia tej kontroli i jest oczywiście to, co się wydarzyło po jej zakończeniu. Tutaj raport ten został opublikowany w styczniu bieżącego roku. Mamy sierpień. Podkreślaliśmy między innymi te działania, które zostały podjęte przez Ministerstwo i przez inne podmioty po zakończeniu kontroli. Natomiast nie możemy dokonywać krytyki ustaleń Kontroli NIK za dany okres objęty kontrolą, mówiąc, że dzisiaj jest inaczej. Taki był stan na ten dzień, kiedy prowadziliśmy czynności, inny był stan na dzień zakończenia czynności kontrolnych i inny stan jest dzisiaj.

Puentując króciutko i troszeczkę żartobliwie, jeżeli mogę sobie na to pozwolić – bo pan minister bardzo negatywnie ocenił na koniec swojej wypowiedzi raport Najwyższej Izby Kontroli – jako przedstawiciel NIK i osoba, która swoje życie, można powiedzieć, poświęciła służbie temu państwu, chcę powiedzieć, że z mojego punktu widzenia o wiele lepszą sytuacją jest, kiedy przedstawiciele jednostek kontrolowanych krytykują nasze ustalenia, ale wdrażają nasze wnioski pokontrolne – a to zostało tutaj również w wypowiedzi pana ministra podkreślone, że wnioski są realizowane – niż gdy występuje sytuacja odwrotna. Dziękuję bardzo.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo serdecznie panu dziękuję. Jeszcze pani Joanna. Bardzo proszę.

Członek Stowarzyszenia ISACA Warszawa Joanna Karczewska:

Dzień dobry. Nazywam się Joanna Karczewska i dzisiaj jestem w podwójnej roli – jak zwykle jako przedstawicielka środowiska, które na co dzień zajmuje się cyberbezpieczeństwem, bezpieczeństwem informacji i ochroną danych osobowych, ale również jako ekspert, który pracował razem z Najwyższą Izbą Kontroli przy omawianych dzisiaj wynikach. Za to dziękuję, był to dla mnie zaszczyt.

To była niezwykła praca, wykorzystałam całe moje doświadczenie zawodowe. W informatyce pracuję ponad 40 lat. Informatyzowałam między innymi dwa banki, ZUS i wiele innych instytucji polskich i zagranicznych.

Natomiast komentując wypowiedzi. Otóż 4 lipca ukazał się raport Banku PKO SA „Czy czujesz się bezpiecznie w Internecie?". Z raportu wynika, że niestety, ale nadal są problemy z uzyskaniem wiedzy na temat cyberprzestępczości. Dobrze, że jest nagranie – i to powiedziałabym, że potwierdzające w 110% wyniki kontroli NIK. Okazuje się, że większość osób czerpie wiedzę od znajomych oraz ogólnie z internetu. Natomiast dużo mniej osób korzysta z kampanii w mediach, a jeszcze mniej zagląda na dedykowane strony internetowe. Zatem niewiele się zmieniło i nadal jest nad czym popracować. To mnie naprawdę zaskoczyło, bo jest mi to niezwykle potrzebne, żeby był jeden dedykowany portal, który ja będę mogła rekomendować, m.in. znakomitym paniom woźnym, z którymi współpracuję w przedszkolach. One też mają telefony komórkowe, też korzystają z internetu. Chciałabym móc im wskazać jedno podstawowe źródło informacji o cyberbezpieczeństwie.

Co do algorytmów zgłaszania, polecam Policji przyjrzeć się francuskiemu rozwiązaniu. Oni mają oddzielny portal. Tam są wręcz podane wskazówki, co przygotować, jak zgłaszać zagrożenia czy też stwierdzone naruszenia bezpieczeństwa i ochrony danych osobowych.

Natomiast co do CERT i podawanych liczb zgłoszeń – czy to jest dużo, czy mało, nie sposób ocenić. Na pewno liczba będzie rosnąć. Sama, jak dostanę e-maila, to zgodnie z waszą prośbą i rekomendacją od razu wysyłam do was i natychmiast kasuję u siebie na komputerze. Zdarzyło mi się, że dostałam później prośbę o przesłanie oryginału i musiałam stwierdzić, że oryginału już nie mam – chcieliście zajrzeć do parametrów wiadomości, ale już nie miałam, bo dla bezpieczeństwa od razu wszystko kasuję ze swojego komputera. Z mojego punktu widzenia jako inspektora ochrony danych, jako osoby, która nadal jest czynna zawodowo, jako certyfikowanego audytora systemów informatycznych, jest naprawdę jeszcze wiele do zrobienia. Czekam na możliwość dalszego komentowania. Polecam moje artykuły, które udostępniam m.in. Komisji. One są dostępne bez ograniczeń w internecie. Proszę czytać na bieżąco, co widzę i jak można coś jeszcze ewentualnie naprawić.

Co do wynagrodzeń, chciałam zwrócić uwagę, że niedawno w Senacie ustępujący i kandydujący prezes Urzędu Ochrony Danych Osobowych skarżył się, że jego urząd nie jest objęty ustawą o wyższych wynagrodzeniach dla osób zajmujących się cyberbezpieczeństwem. Może warto jeszcze dokonać analizy, gdzie można wspomóc? Przecież to jest bardzo ważny urząd. Sami wydają rekomendacje i nakładają kary administracyjne za brak bezpieczeństwa informacji. Większość kar ostatnio to jest...

Przewodniczący poseł Grzegorz Napieralski (KO):

Przepraszam, że przerwę. A Policja w tym jest? Jest. OK.

Członek Stowarzyszenia ISACA Warszawa Joanna Karczewska:

Na ten temat się nie wypowiadam. Natomiast wiem, że prezes UODO się skarży, że nie jest w stanie zapłacić swoim pracownikom odpowiednich kwot. A z kolei sam urząd przecież ocenia innych – co jest ewidentnym dysonansem.

To, co pan poseł powiedział, potwierdza, że jeszcze bardzo dużo osób potrzebuje wiedzy. Skoro sami przedsiębiorcy… Bo małe i średnie przedsiębiorstwa są naprawdę zaniedbane i też by im się przydał jeden, jedyny, najważniejszy portal – tak jak mają Francuzi, tak jak mają Brytyjczycy. Ostatnio zaglądałam na strony Papui-Nowej Gwinei. Oni też mają zespół, który zajmuje się cyberbezpieczeństwem. Ale stwierdzili, że oni sami nie są w stanie tematu ogarnąć, że tak powiem, w związku z tym korzystają z pomocy Austra-

lii i Nowej Zelandii. Można więc też szukać natchnienia i pomocy gdzie indziej. Natomiast na pewno jesteśmy cały czas na początku drogi, a nie w dobrym punkcie, który można ocenić pozytywnie. Tak mówię z mojego doświadczenia. Dziękuję.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję za ten głos merytoryczny. Pan dyrektor? Proszę bardzo, panie dyrektorze.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji Marcin Wysocki:

Bardzo dziękuję, panie przewodniczący. Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji.

Chciałbym uzupełnić dyskusję o dwa wątki. Witryna jest bardzo ważna, żeby znaleźć te informacje, najlepiej w jednym miejscu. Ale nie tylko. Chciałbym wskazać, że wśród akcji promocyjnych jest również spot zachęcający do tego, żeby złośliwe SMS-y czy komunikację podszywającą się zgłaszać do NASK. Był na przykład emitowany podczas tak zwanego prime time'u przed rozpoczęciem meczu polskiej reprezentacji podczas ostatniego mundialu…

Natomiast co do wynagradzania ekspertów z Policji zajmujących się cyberbezpieczeństwem – oczywiście, że tak, policjantom są wypłacane środki na ten cel. Natomiast są to zadania z zakresu bezpieczeństwa. W obecnym kształcie one nie obejmują – lub jest wątpliwość, czy obejmują – katalogu ścigania przestępstw z zakresu cyberbezpieczeństwa. Taka szersza kategoria… Taka poprawka miała być zgłoszona w związku z procedowaniem nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, o której rozmawialiśmy wcześniej na posiedzeniu. Bardzo dziękuję, panie przewodniczący.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję za te wyjaśnienia, panie dyrektorze. Skoro pan mówi trochę o tej kampanii społecznej, to ja bym się zastanowił… Nie ma chyba nic ważniejszego niż dobre poinformowanie Polek i Polaków o tym, jak się chronić przed tymi atakami. Ich będzie coraz więcej. Coraz więcej będzie się przenosić z realnego świata do sieci.

Natomiast poddaję pod uwagę takie pomysły, panie dyrektorze – żeby to przedyskutować i znaleźć na to pieniądze w budżecie. Po pierwsze mamy telewizje śniadaniowe, które są w dużej mierze oglądane przez ludzi, którzy czerpią z tego też wiedzę. Taką dosyć rzetelną. Stacje starają się robić te programy dosyć rzetelnie. Ta wiedza jest oczywiście w różnym zakresie – od gotowania po ubiór. Ale gdyby tam w przystępny sposób – gdyby się z telewizjami współpracowało – takie tematy się pojawiały, myślę, że to by bardzo pomogło. To jest rzecz pierwsza, panie dyrektorze.

Rzecz druga to jest kwestia dotycząca tego, na co rząd ma na pewno wpływ i pieniądze –seriale. Jeżeli spojrzymy na ilość oglądanych seriali przez Polki i Polaków, to można powiedzieć, że połowa Polski ogląda seriale. Około 20 milionów ludzi dziennie ogląda różne seriale. Można dzisiaj zaproponować stacjom telewizyjnym, które wykupują takie seriale – trzeba by stworzyć jakiś fundusz, musielibyśmy się nad tym zastanowić – że dołożycie się do takiego serialu, jeżeli w serialu pojawiać się będą wątki uczące cyberbezpieczeństwa. W jakiś sposób. Kiedyś mówiliśmy o tym, jak trzeba się zaszczepić… To już od reżysera i scenarzystów zależy, nie ode mnie. Ale ja bym takie rzeczy na pewno wziął pod uwagę. Można zobaczyć, co się w Sejmie działo. Przeszliśmy szkolenie w parlamencie, ale jestem święcie przekonany, że jeszcze by nam się trochę wiedzy przydało. A często po prostu oglądając coś takiego, moglibyśmy… Oczywiście prime time'y są ważne, a także informacje, kampanie społeczne... Tylko przy natłoku reklam, panie dyrektorze, też mamy ograniczoną percepcję dla takich rzeczy. Fajnie, że coś mówią, o SMS-ach, to jest ciekawe, ale… To jest istotne. Natomiast proszę zastanowić się nad takimi rzeczami. Wszystkie telewizje prywatne i państwowe mają swoje kanały informacyjne. TVP Info, TVN24, Polsat News… Można z nimi też porozmawiać, żeby w pasmach informacyjnych też takie tematy by się pojawiały. Zapraszałoby się na przykład polityków, ekspertów, przedstawicieli rządu, żeby taka dyskusja się odbywała – nie na zasadzie konfrontacji politycznej. Bo to też wzbudzi zainteresowanie tematem. Jak tego nie zrobimy, panie dyrektorze, to naprawdę może wydarzyć się wiele różnych rzeczy i możemy mieć z nimi problem.

Nie ma zgłoszeń do dyskusji. Zamykam dyskusję. Bardzo dziękuję wszystkim, którzy byli z nami dzisiaj na posiedzeniu Komisji.

Zamykam posiedzenie. Wszystkiego dobrego i do zobaczenia.